Chapter 10
BMAR – Blockchain for Medication Administration Records

I. Mitchell and S. Hara

Abstract Medication Administration Records are crucial documents in the care and quality offered to service users. Audits will inspect MAR sheets and these will form a significant impact on the outcome of Medication Management. This impact will be combined with inspections of registered hospitals, care and residential homes across the healthcare profession. The proposal is to build a prototype using blockchain technology to implement MAR sheets, essentially building a blockchain application that stores electronic health records (EHR). The use of permissioned blockchain technology provides confidentiality and trust with the auditors (e.g., CQC). The prototype is tested on two scenarios and results are encouraging. The results indicate that reminders can be sent to healthcare professionals and other consequences of the implementation of EHR and *permissioned* blockchain.

Keywords Medical Administration Records (MAR) · Electronic Health Records (EHR) · Care Quality Commission (CQC) · Blockchain

10.1 Introduction

The medication administration is an important procedure for ensuring the high quality of care delivered by healthcare professionals. Healthcare providers use a Medication Administration Records sheet to record the information about the administration of medicine by healthcare professionals to its service users.

Many systems have been developed and significant improvements to medication management can be achieved by using automated systems (Bates et al. 1998) and mild improvements to medication management can be achieved by sending reminders to healthcare professionals (Bennett et al. 2003). So, the design, development and implementation of an automated system for the completion of MAR sheets is

I. Mitchell (✉) · S. Hara
Middlesex University, London, UK
e-mail: I.Mitchell@mdx.ac.uk; s.hara@mdx.ac.uk

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_10

not new, what is new is the ability to implement MAR sheets using blockchain technology and the advantages it may bring.

It is difficult to write a paper on blockchain without mentioning BitCoin (Nakamoto 2008) since it is the predecessor of all blockchain applications. Bitcoin uses blockchain to record transactions between two or more Bitcoin wallets. So what is blockchain? In simple terms, it is an append-only encrypted ledger, that requires consensus to be updated. There are two important terms here that make blockchain ideal for auditability, which are: append-only – means that data added to the blockchain is immutable, without considerable effort it cannot be changed; and consensus – there is a decentralised component that requires all nodes in the network to have consensus before updating, this promotes trust between parties in the network.

Tokens, or coins, are often used when items of value are exchanged, in many applications tokens are not required since items of value are not exchange. Whilst information is exchanged in BMAR, it does not have monetary value and therefore no tokens are required – BMAR will be tokenless.

Finally, there are two important differences in the implementation of blockchain applications, these are *permissioned and* permissionless. Permissionless, allows the nodes, that are part of a consensus, to be added without permission of the system. This is compared with permissioned blockchain that only allows authorised nodes to be added to the network – this has the added benefit of keeping data confidential to only those authorised nodes and further restrictions can be added to individual users.

In summary, the application developed is a tokenless permissioned blockchain, this results in data being append-only and immutable, which is ideal for audits, and keeps data confidential due to the encryption used in the blockchain technology. The implementation will be carried out using Hyperledger Fabric and Composer (Hyperledger architecture 2017, 2018) and results and recommendations are reported in Sects. 10.3 and 10.5, respectively.

10.2 Design

There are some key transactions of information in Medical management, which are as follows:

Prescription
A qualified individual has to prescribed the medication and dosage, e.g. a Medical Doctor.

Administration
A qualified individual has to administer the medication, e.g. Nurse.

Management
A manager would oversee the schedules, delegate appropriate staff to the administration of medication, and register service users with the Healthcare Provider.

Observe
Administration of controlled substances requires observation of the administrator that provides a witness. This account is also recorded.

Audit
External and Internal Audits occurs

There are key individuals involved in the transactions of information in BMAR application. For the scope of this application this includes:

Doctor
Ability to *prescribe* medication to patients. There are many individuals that can prescribe medication, but for the scope of this paper, the individual will be referred to as a Doctor.

Nurse
Ability to administer medication to patients. There are many individuals that are qualified to complete this task and come under the umbrella term, healthcare professionals.

Patient
Receives medication and uses the services of the home, often referred to as a resident or service user.

Home
The location of the patient, could be a hospital or a care home. The home is inspected and 1 or more patients reside there. The home offers a service and is often referred to as a healthcare provider.

Auditor
Qualified individual that inspects the home and reports if it is fit for purpose. Typically from an external agency, e.g., in the UK the Care Quality Commission (CQC).

Manager
Manager of the home and responsible for the quality of care given to patients.

Witness
Controlled substances require observation of the individual administering the medication. Usually, a manager or a different healthcare professional.

With the above terms of reference, Fig. 10.1 illustrates the interaction between users and the system. Whilst it is appreciated that not all healthcare professionals who administer medication have Nurse qualifications, it is done for simplicity and understanding, likewise for other users in the system.

The five use cases coincide with the five stages identified in the list above. These are the transactions and is the data stored on the network. There is a worry about such data being immutable and therefore care has to be taken about the rights of individuals to remove data (Council of European Union 2018). Data on the blockchain cannot be removed, so transactions would have to store data that is at least pseudo-anonymised. The data stored in the system, registries referring to unique

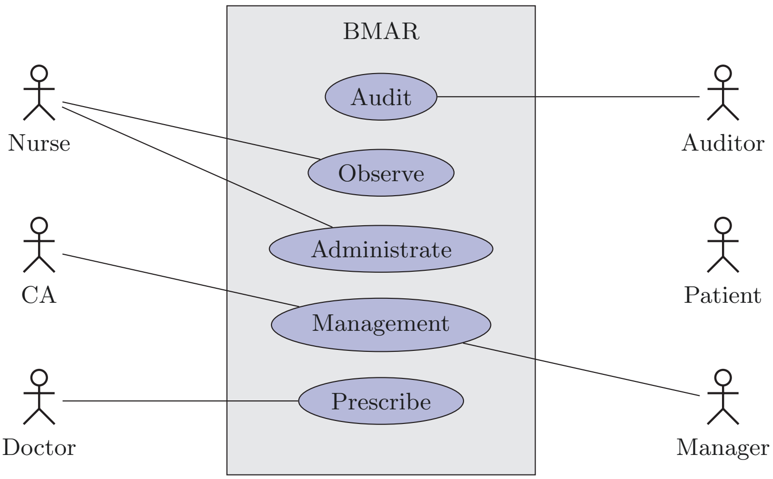


Fig. 10.1 Use: Case diagram for BMAR. Central Authority (CA) is a NHS trust, or private healthcare provider

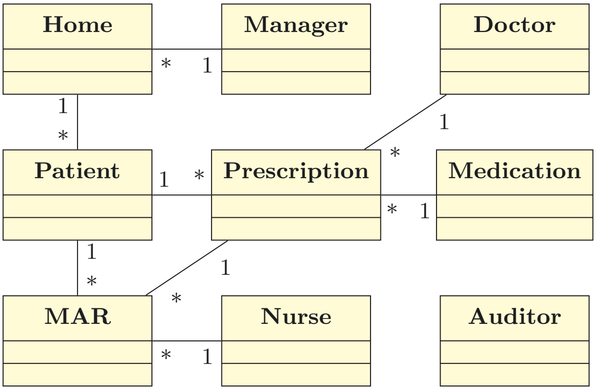


Fig. 10.2 Simplified class diagram for BMAR, omitting attributes

identifiers on the blockchain, can be removed and thus protect the rights of individuals. However, the security of data on permissioned blockchain applications is encrypted and secure, see (Gupta 2018, ch. 5) for further details (Fig. 10.2).

10.2.1 Data Protection

In the UK all e-Health applications need to comply with the seven Caldicott principles (Caldicott 2013). BMAR would be no exception and the following has been considered during the design of the system:

1. Justify the purpose: MAR sheets already exist and data is being collected on service-users and their medication administration. The justification is to design an automatic system to complete the task and store the data electronically for future audits.
2. Don't use personal confidential data unless it is absolutely necessary: The transactions are immutable and therefore considerable care has been taken to ensure that the minimum amount of data is included. The transactions are designed to include no personal information to identify participants, including healthcare professionals and service users. Permissioned blockchain technology is highly secure and encrypted, therefore protecting data.
3. Use the minimum necessary personal confidential data: De-duplication of data are kept to a minimum in the design. Data on both the participants and the assets, stored in the registries, have low volatility, and whilst changes occur it is not every second. However, data transferred in the transactions, stored in the blockchain, have high volatility.
4. Access to personal confidential data should be on a strict need-to-know basis: Access control language allows only certain users to access certain registries and therefore access is strictly on a need to know basis. Role-based attribute control (RBAC) (Richard Kuhn et al. 2010) is employed to ensure correct and appropriate access.
5. Everyone with access to personal confidential data should be aware of their responsibilities: Training at induction and regular supervision would ensure that all staff are aware of their responsibilities, something that is outside the scope of the system.
6. Comply with the law: BMAR would meet with current laws and regulations about sharing and using e-Health information.
7. The duty to share information can be as important as the duty to protect patient confidentiality: At all times patient confidentiality is kept. The ingenuity of blockchain not only allows and promotes sharing of data but also extends it. For example, a Healthcare Provider, X, intends to join the BMAR blockchain, which already hosts 20 other Healthcare Providers. The disintermediatory nature (Gaur et al. 2018) allows new organisations to join the blockchain without compromising existing data. So, our new Healthcare Provider, X, can join BMAR without viewing MAR sheets from other organisations, allowing its own staff to manage its own information, GPs to complete prescription information, and, more importantly, seamlessly allow auditors, such as the Care Quality Commission (CQC) to view their MAR sheets.

10.2.2 Prescription

The scope of BMAR is not to include prescriptions, however, it is appreciated that a qualified individual, e.g., a medical doctor, would have to prescribe medication. Figure 10.3 shows a simplified prescription process, the prescriber has to write one

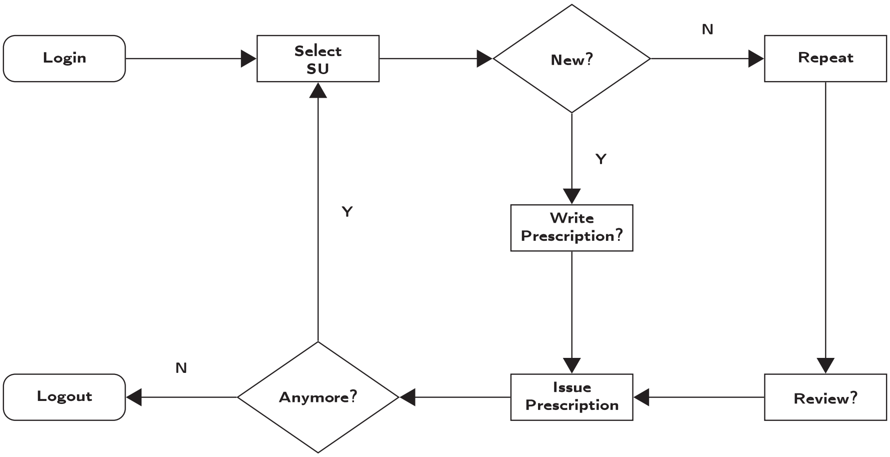


Fig. 10.3 Flowchart for completion of prescription. (Note, the scope of this application is not to implement the prescription processes and procedures and therefore simplified. Abbreviation: *SU* Service User)

medication per prescription. This means that an individual requiring multiple medications would receive multiple prescriptions.

The flowcharts in Fig. 10.3 is by no means to replace the expertise available to the GP, this goes for the other flowcharts. However, the flowcharts do cover the process of issuing a prescription, and in particular looks at a selection of a service user and issuing repeat or new prescriptions. Once complete the GP either selects another, or the same service-user to issue another prescription. Such processes do not simulate the process of issuing multiple prescriptions and would annoy the user. This is the process, the procedure for issuing multiple prescriptions could easily be completed concurrently.

10.2.3 Management

There are many managerial tasks that could be included here, two were chosen to demonstrate that permissioned blockchain has the capabilities to facilitate such tasks. Two tasks were chosen and discussed below.

10.2.3.1 Assign Key Worker

Whilst outside the scope of this prototype, it is recognised that key workers are assigned to service users and have important responsibilities. Assigning a key worker is a managerial duty and is demonstrated here to show how blockchain applications can accommodate such processes as a transaction.

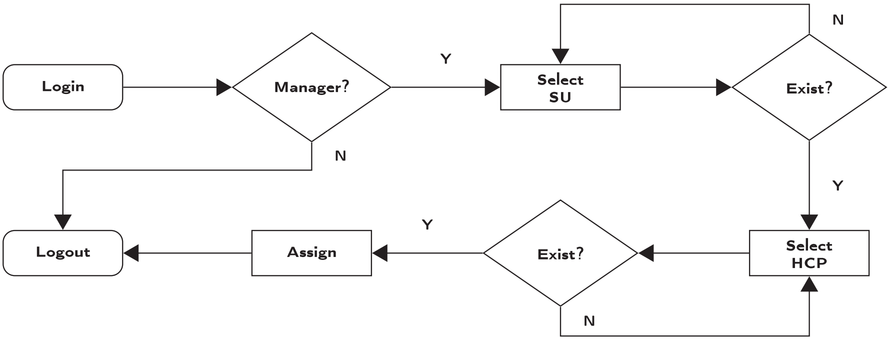


Fig. 10.4 Flowchart for completion of assigning keyworker to service-user (Patient). (Abbreviations: *SU* Service User, *HCP* Healthcare Professional)

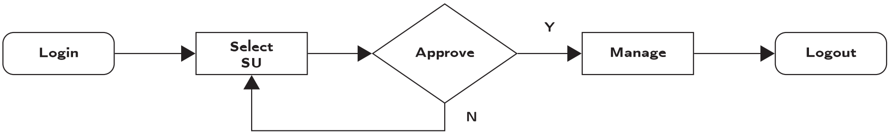


Fig. 10.5 Flowchart for registering a service-user with a healthcare provider. (Abbreviations: *SU* Service User)

The procedure is simple and shown in Fig. 10.4, only a manager can have access to the transaction to assign a healthcare professional as a key worker to a service user (patient). Whilst comparisons can be made to databases, blockchain applications are different and checks should be completed to ensure that both the service user and healthcare professional exist. Once the necessary checks are completed the assignment of the key worker is complete and the manager can log out, or assign another key worker.

Each of these assignments is included on the blockchain, this includes the date, time, manager, service-user and healthcare professional.

10.2.3.2 Register Service-User with Home

The flowchart in Fig. 10.5 illustrates the process of registering a service user with a healthcare provider. The issue here is one of access control and cannot be shown on a simplified flowchart, as soon as the service-user is registered, the access control to their records changes. The healthcare provider they were moving from relinquishes access control to the individual's records, whilst the healthcare provider they are moving to gains access control to the individual's records.

A central authority issues the approval, in the case where the service user is moving between different healthcare providers this could be an NHS Trust or GP. In the case where the service user is moving to a different residence owned by the same healthcare provider, this authority would come from the area manager for that organisation.

The smart contract would be enacted when the move of the service user has been approved. Using ABAC (Vincent et al. 2014), which is support by Hyperledger Fabric, the access control is changed on the attributes of the participants and assets, so the implementation is seamless and requires no further work. For example, the healthcare professional administrating medication requires access to the service user's records, for this the healthcare professional needs the required attributes to have 'READ' access to these records. Put simply, the residence would have to be equal for both the service user and the healthcare professional, further attributes can be added, such as the healthcare professional has to be registered, qualified and if there is a system to clock-in then confirmed that he or she is on-site. Hyperledger's Access Control Language (ACL) can easily implement such conditions and ensure that confidentiality is not breached.

Two additional systems have been introduced here, a central authority to approve the move of the service user, and a system to monitor employees when they are present at the residence (all visitors and employees have to register when they are enter and leave the premises). Permissioned blockchain can easily allow additional authenticated users with limited access control, even of a non-person entity (NPE) variety, as in the case of a clock-in system.

10.2.4 Medical Administration

Completion of the Medical Administration Records Sheet is an important task for the welfare of the service-user. BMAR does not make any claims that it improves this procedure, merely that it can be implemented and all actions recorded without modification. In fact, caution should be taken if this was implemented since there are effects of introducing automated systems, e.g., post-completion error, whereby the appropriately qualified Healthcare Professional completes the form, but forgets to complete the task and administer the medication, see (Yau Wai et al. 2005) for further information.

Whilst caution and further research should be taken, there is evidence that the (Bates et al. 1998; Bennett et al. 2003), that medication administration could benefit from the introduction of such technologies (Fig. 10.6).

10.2.5 Medical Observation

As expected the process for observation of medication is similar to the administration of medication and is shown in Fig. 10.7. This process is mandatory for all controlled drugs. After logging-in the observer selects the correct service user and

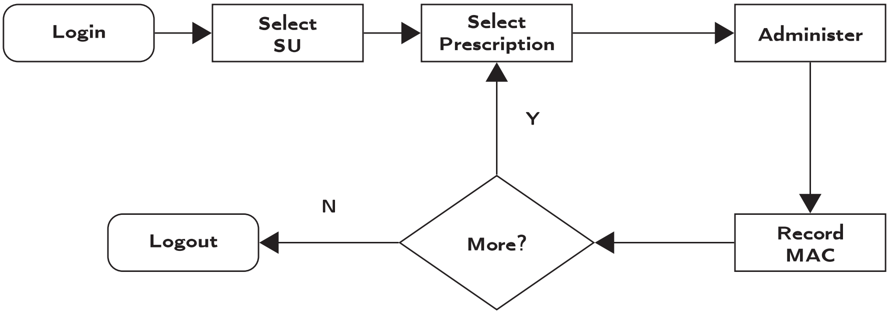


Fig. 10.6 Flowchart for completion of MAR sheet. (Abbreviations: *SU* Service User, *MAC* Medication Administer Code, can be values such as taken, refused, vomit, sleeping or absent)

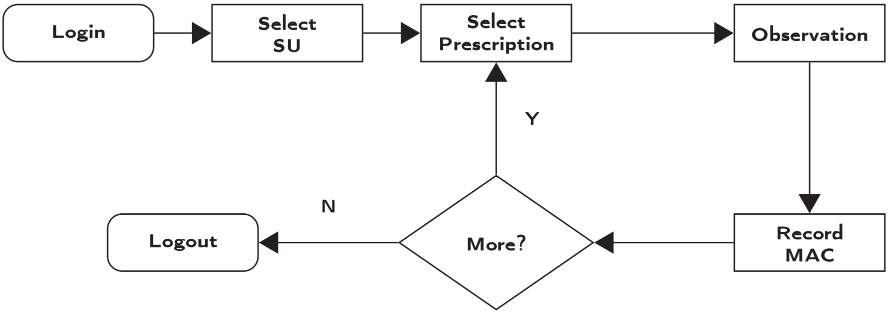


Fig. 10.7 Flowchart for completion of observation for MAR sheet. (Abbreviations: *SU* Service User, *MAC* Medication Administer Code, can be values such as taken, refused, vomit, sleeping or absent)

associated prescription, and this would be completed in parallel with the person administrating the medication. Once the medication has been administered the observer enters the correct MAC. If there are multiple prescriptions then the process is repeated.

There are some anomalies that the audit can reveal, for example when an observation is recorded as a transaction on the blockchain before the administration. This, and other queries are discussed in Sect. 10.2.6 audits.

10.2.6 Audit and Security

An audit agency, such as the Care Quality Commission, would have ‘READ’ access to all records and transactions on the system. Predefined queries can be completed for each healthcare provider, grouped by residence and service user. Often the accumulation of these reports makes it difficult to find anomalies, however, search algorithms can be deployed and queries can be designed to find any issues that may arise. For example, a MAR sheet error can be self-audited and left to the expertise of the auditor to question the manager of the care home. This is nothing new, however, the innovative part is the use of blockchain technologies to ensure a disintermediatory append-only ledger of MAR sheets, which makes it impossible to retrospectively delete or correct. There are arguments about a 51% attacks (Bastiaan 2015), which are theoretical and often discussed with permissionless blockchain technology. Firstly, with permissioned blockchain, the likelihood of such an attack is diminished further since all nodes in the network are authenticated by an access control layer. Secondly, such an attack would require changing more than $\frac{2}{3}$ of nodes since the consensus algorithm, PBFT (Castro et al. 1999), used requires a higher percentage of agreement. This vulnerability of permissioned blockchain has an extremely low probability of success, nevertheless, it is mathematically possible and discussed in (Zyskind et al. 2015). The transaction process is fully encrypted and Hyperledger Fabric requires participants to be certified and therefore providing a security infrastructure for authorisation and authentication, see (Cachin 2016) for more details.

10.3 Results

The access latency for transactions is instantaneous, for BMAR there are relatively small amounts of data, <1Kbyte, uploaded to the permissioned blockchain and the delay is negligent. Hyperledger has demonstrated elsewhere with documents (>10Kbyte) the access latency is less than 2 s (Androulaki et al. 2018). The latency has not been fully tested, however, other implementations (Thakkar et al. 2018) indicate that access latency is dependent on transactions per second and block size.

The tests were mainly completed to see how the blockchain could be accessed and processed by key personnel involved in the care and support of a service-user. The development and implementation gave a valuable and insightful understanding of the nuances of administration of medication process. The decision to separate data was based on some rationale regarding access to data, e.g. should auditors be able to identify a service-user or healthcare professional by name? Is there a need for an auditor, when the system can audit itself? These questions are visited in the conclusions. The data stored in asset and participant registries has restricted access.

10.3.1 Prescription

The prescription process has been simplified, but it is possible that the details provided below can be provided from other systems used by the healthcare profession. The prescription process is outside the scope of this project, and essentially the list

```
1  =========== REGSITRY ============
2  {
3    "$class": "org.bmar.net.Prescription",
4    "ID": "5579",
5    "Patient": "resource:org.bmar.net.SU#S111",
6    "PrescribedMedication": "resource:org.bmar.net.Medication#111",
7    "initialisation": "2018-10-25T17:26:56.674Z",
8    "Form": "Pill",
9    "Route": "Oral",
10   "Controlled": false,
11   "Duration": "4",
12   "Dose": "25",
13   "Quantity": 1,
14   "Instructions": "One (1) tablet two (2) times a day"
15 }
16 =========== TRANSACTION =============
17 {
18  "$class": "org.bmar.net.Prescribe",
19  "actualPrescription": "resource:org.bmar.net.Prescription#5579",
20  "transactionId": "91a39021-d1b7-4c8e-9eb2-540b82e641fe",
21  "timestamp": "2018-10-25T17:30:29.706Z"
22 }
```

Fig. 10.8 Transaction for prescription, output shows entry for a prescription in the asset registry, 'Prescription'

of information provided in Fig. 10.8 is minimal requirement. The information can only be provided by a qualified GP or equivalent, and 'READ' access is given to other participants in the system. The transaction records the date and the participant who issued the prescription (not shown). A quick breakdown of the code in Fig. 10.8 shows on line 4 a unique identifier for the prescription, line 5 the unique identifier for the service user, line 6 the unique identifier of the medication and lines 7–14 the details of the prescription.

10.3.2 Medical Administration

Records in the registry can be altered, every update of the records in the registry is written to the blockchain. So, all changes to assets and participants are recorded on the blockchain in perpetuity. Medical Administration is no exception and is conducive to blockchain technology due to its auditable nature.

Lines 1–32 in Fig. 10.9 shows the result of a change in the records for an administration of a prescription, '5579', to a service-user, 'S111', at a Healthcare Provider, 'H1'. Line 29 indicates that actual medication administration code (MAC) recorded by the Healthcare professional was 'taken'. Line 30 indicates that this was not confirmed by the observer, which is completed by a different transaction and updated accordingly.

There are some important omissions of information that are required. This vital information is stored in the associated transaction display between lines 34–42. Here the relationship to the service user is stored, 'S111' (line 36), the prescription, '5579', the timestamp and finally, the transaction ID. The healthcare professional completing the medication administration is recorded as access on the blockchain, not shown here.

```
 1 =========== REGSITRY =============
 2 {
 3   "$class": "org.bmar.net.MAR",
 4   "time": "1540490058276",
 5   "actualPrescribedMed": {
 6     "$class": "org.bmar.net.Prescription",
 7     "ID": "5579",
 8     "Patient": "resource:org.bmar.net.SU#S111",
 9     "PrescribedMedication": "resource:org.bmar.net.Medication#111",
10     "initialisation": "2018-10-25T17:26:56.674Z",
11     "Form": "Pill",
12     "Route": "Oral",
13     "Controlled": false,
14     "Duration": "4",
15     "Dose": "25",
16     "Quantity": 1,
17     "Interval": 0,
18     "Instructions": "One (1) tablet two (2) times a day"
19   },
20   "actualPatient": {
21     "$class": "org.bmar.net.SU",
22     "ID": "S111",
23     "firstName": "S",
24     "lastName": "U",
25     "Allergies": "none",
26     "DoB": "1991-08-10T00:00:00.000Z",
27     "KeyWorker": "resource:org.bmar.net.HCP#HP111",
28     "Home": "resource:org.bmar.net.HealthCareProvider#H1"
29   },
30   "actualMAC": "taken",
31   "ObservedMAC": "unconfirmed"
32 }
33 =========== TRANSACTION =============
34 {
35  "$class": "org.bmar.net.Administer",
36  "Patient": "resource:org.bmar.net.SU#S111",
37  "actualPrescribedMed": "resource:org.bmar.net.Prescription#5579",
38  "time": "2018-10-25T20:02:29.832Z",
39  "recordedMAC": "taken",
40  "transactionId": "7d919a4c-2c71-4ea6-a073-deffb3e19fc3",
41  "timestamp": "2018-10-25T20:03:15.236Z"
42 }
```

Fig. 10.9 Ouput for transaction for administration. Top half is stored on registry, the bottom half is stored on blockchain

10.3.3 Observation

Lines 2–13 in Fig. 10.10 shows the changes to the asset as a result of the observation transaction. Lines 6 and 9 are the same information as the information stored in the administration transaction in Fig. 10.9 and for brevity not repeated here. On line 11 the recorded MAC is entered as ‘taken’ as entered in a previous transaction. The important change is to compare lines 31 and 12 in Figs. 10.9 and 10.10, respectively. The value assigned to the attribute, ‘ObservedMAC’ has changed from ‘unconfirmed’ to ‘confirmed’, which matches the value in the transaction (line 18 in Fig. 10.10. In the transaction, the timestamp is recorded at, ‘2018-10-25T20:25:02.478Z’, some 22 min are the administration of the medication.

The ID of the individual MAR was completed as converting a timestamp to a string, in fact on line 4 in Fig. 10.10 the asset attribute name is ‘time’. In a system where there are potentially millions of MAR entries, this could be a little simplistic, although it works for our prototype. In such situations, Hyperledger suggests to merge and split attributes to maintain their unique identity, so an obvious candidate is the prescription ID.

Finally, not shown in the transaction is the identity of the healthcare professional conducting the observation, this is included on the blockchain and not shown here.

```
1  =========== REGSITRY =============
2  {
3    "$class": "org.bmar.net.MAR",
4    "time": "1540490058276",
5    "actualPrescribedMed": {
6            ...........
7      },
8    "actualPatient": {
9            ...........
10   },
11   "actualMAC": "taken",
12   "ObservedMAC": "taken"
13 }
14 =========== TRANSACTION =============
15 {
16  "$class": "org.bmar.net.Observe",
17  "unconfirmedMAR": "1540490058276",
18  "ObservedMAC": "taken",
19  "transactionId": "22b1d98c-70e2-46c6-83a2-9637ad36698e",
20  "timestamp": "2018-10-25T20:25:02.478Z"
21 }
```

Fig. 10.10 Ouput for transaction for observation. For brevity, the information in the ‘actualPrescribedMed’ and ‘actualPatient’ are not displayed here and are the same as in Fig. 10.8

10.4 Management

Access to management functions would be restricted to Managers and entirely role-based. However, there are the attributes of the asset or participant being managed to take into consideration. These two options demonstrate the participant management.

Lines 2–11 in Fig. 10.11 shows the data stored in the blockchain as a result of the transaction. The service user, identified as ‘S444’ (line 4), has been assigned a key worker ‘HP333’ (line 9) and registered at a healthcare provider, identified as ‘H1’ (line 10).

The transaction of the service user to the healthcare provider is shown in lines 13–18 in Fig. 10.10. An existing service user and home have been selected. The transaction timestamp is on line 17 and should pre-date the following transaction.

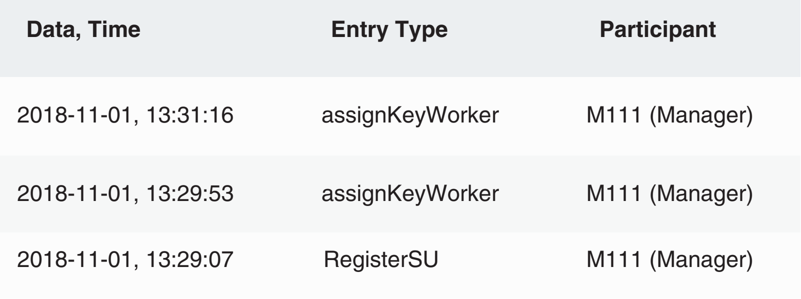
The transaction of assigning a key worker to the service user is shown in lines 20–26 in Fig. 10.10. The pre-conditions for this is that the service user selected has to be registered to a healthcare provider managed by the manager completing the transaction, and the key worker is a healthcare professional working at the same healthcare provider. The transaction timestamp is on line 25 and post-dates registering a service user with a healthcare provider.

10.4.1 Audit

Various queries can be set up to produce reports for auditors. Figure 10.12 illustrates one of many views an auditor may have, here is a sample of the transactions made for management. The key problem in the above examples is seeing who completed the transactions, here by simply matching the timestamps reveals who submitted the transaction:

```
1  ===========REGISTRY============
2  {
3    "$class": "org.bmar.net.SU",
4    "ID": "S444",
5    "firstName": "B",
6    "lastName": "C",
7    "Allergies": "",
8    "DoB": "1994-07-25T00:00:00.000Z",
9    "KeyWorker": "resource:org.bmar.net.HCP#HP333",
10   "Home": "resource:org.bmar.net.HealthCareProvider#H1"
11 }
12 ===========REGISTER SU TRANSACTION============
13 {
14  "$class": "org.bmar.net.RegisterSU",
15  "Patient": "resource:org.bmar.net.SU#S444",
16  "Home": "resource:org.bmar.net.HealthCareProvider#H1",
17  "transactionId": "4b25df90-5dec-47e0-b58d-511908225343",
18  "timestamp": "2018-11-01T13:29:07.629Z"
19 }
20 ===========ASSIGN KEYWORKER TRANSACTION============
21 {
22  "$class": "org.bmar.net.assignKeyWorker",
23  "newKeyWorker": "resource:org.bmar.net.HCP#HP333",
24  "Patient": "resource:org.bmar.net.SU#S444",
25  "transactionId": "e2d55441-813e-4785-8e6c-04b44bca5818",
26  "timestamp": "2018-11-01T13:31:16.812Z"
27 }
```

Fig. 10.11 Output for management transactions. Registry shows data held on particpant after two transactions completed below



Data, Time	Entry Type	Participant
2018-11-01, 13:31:16	assignKeyWorker	M111 (Manager)
2018-11-01, 13:29:53	assignKeyWorker	M111 (Manager)
2018-11-01, 13:29:07	RegisterSU	M111 (Manager)

Fig. 10.12 Audit view for transactions

2018-11-01T13:29:07.629Z:

Matching this transaction from Fig. 10.11 (line 18) to Fig. 10.12 shows that the transaction was to ‘RegisterSU’ and conducted by ‘M111(Manager)’.

2018-11-01T13:31:16.812Z:

Matching this transaction from Fig. 10.11 (line 26) to Fig. 10.12 shows that the transaction was to ‘assignKeyWorker’ and conducted by ‘M111(Manager)’.

10.5 Conclusions

There are many proposed blockchain healthcare systems, e.g., see (Azaria et al. 2016; Griggs et al. 2018; Vithanwattana et al. 2017; Zhang et al. 2017). However, whilst these proposed systems are all meaningful, the prototype for BMAR is for a different application and designed for the recording and auditing of medication administration records.

All Caldicott principles have been considered in the design of this application and meaningful-use would be the reduction of MAR sheet errors with the overall intention of improving health services and safeguarding vulnerable adults. The permissioned blockchain application provides the security and privacy required for health informatics. The data is permanent and immutable, which makes it an ideal technical solution to the MAR sheet problem.

During the design and implementation stages, it was considered that much of the data will already be available as EHR. It is highly likely that such an implementation would require the use of EHR in an existing database and therefore it is recommended to keep registries relatively static since it is the transactions that change. Such designs lead to keeping databases relatively static and a reliance on blockchain for transactions and change. As a recommendation, when designing a blockchain application it is useful to identify transactions. As yet, there is no standard modelling technique for blockchain and therefore remains a challenge in designing applications. It is recommended that robust modelling techniques are required for building blockchain applications, especially for the modelling and differentiation between transactional, asset and participant data.

From the prototype of BMAR the benefits of using blockchain to manage EHR are as follows:

- Disintermediation is often referred to as the 'removal of the middleman' (Gaur et al. 2018, ch. 1). One of the many promises of permissionless blockchain is the to complete financial transactions without the need of a central banking authority. Permissioned blockchain is no exception and aims to reduce the number of intermediaries between producer and consumer. Whilst BMAR may not have many intermediaries, the process of integration of existing services does not pose a problem.
- Prevention and reduction of medication administration errors. Further research would be required for evidence that BMAR would reduce medication administration errors, however, similar studies (Bates et al. 1998; Bennett et al. 2003) give supporting evidence that medication administration errors can be reduced by the introduction of automated systems. The prevention would come in the form of sending reminders to appropriate healthcare professionals that an administration of medication is due.
- Integrity of EHR. BMAR requires generates a report of MAR sheets, inspected by quality assurance agencies (e.g. CQC) and produced by a healthcare agency. Normally, the inspection would be completed by paper and there would be an issue of trust. Unlikely as it is, physical MAR sheets are designed as append-only, which is why permissioned blockchain are so apt as a technological solution. However, there is only one MAR sheet that normally covers a week for each service-user, and it is not inconceivable for this paperwork to be exposed to the temptation to adjust or rewrite them given the correct circumstances. There has to be an element of trust between the auditor and the healthcare provider to assess

the integrity of the information provided. With permissioned blockchain, even given the correct circumstances the ability to make any amendments to the form retrospectively is virtually impossible. The integrity of the EHR generated by BMAR is to be trusted by all parties.
- Cost in Health Information Technology (HIT) has mixed reviews, with many claiming the high costs and investment (Adler-Milstein et al. 2011) in healthcare systems simply do not deliver. This is often referred to as the productivity paradox (Bui et al. 2018). Nevertheless, there are examples of closed studies that report immediate benefits of HIT (Bates et al. 1998; Bennett et al. 2003). BMAR is to implement a prototype for a blockchain application for MAR sheets and report on self-auditing and reminders sent to assigned staff.
- Interdependency between agencies in the healthcare sector is high. At its best, this can affect cost, with duplicate tests for patients issued by different physicians due to ‘information blocking’, whereby physicians do not have sufficient privileges to access data from other organisations (Azaria et al. 2016). At its worse provide opportunities for rogue physicians to exploit the system. Even for the production of MAR sheets, there is some interdependency between healthcare provider, primary carer and auditors, see principle 7 of Caldicott. Blockchain not only provides a technical solution but in addition provides a system whereby the other interdependent agencies can trust each other’s information.
- Security and Integrity of personal data. In BMAR there is pseudo-anonymous data stored in transactions, and personal and confidential data about service users stored in the registries. With de-anonymity algorithms, e.g., (De Montjoye et al. 2013), and enough reference points pseudo-anonymised data can easily be used to identify individuals. All data needs protection and permissioned blockchain provides the security and ensures the integrity of the data, see (Gupta 2018, ch. 5) for further details.
- Auditability of MAR sheets. Blockchain provides transparent governance and/or auditing. Viewing information in reports generated by a system can be difficult to search. BMAR can assist this since it has the information when medication is to be administered and to who. Therefore, it can self-regulate and highlight errors, essentially highlight errors after reminders have been sent. The auditing agency can review the generated reports at any time and then look into further details as to why there are MAR errors. BMAR is not going to replace the expertise of the individuals but simply give individuals the information required to complete an inspection.

The prototype for BMAR requires further research and development, however, for the reasons above the introduction of such a system would benefit healthcare professionals, healthcare providers and service users.

Acknowledgements The authors would like to thank the invaluable information gain from interviewing healthcare professionals in the design and implementation of BMAR.

Competing Interests None identified.

References

Adler-Milstein J, Bates DW, Jha AK (2011) A survey of health information exchange organizations in the united states: implications for meaningful use. Ann Intern Med 154(10):666–671

Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth eurosys conference. ACM, New York, p 30

Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: using blockchain for medical data access and permission management. In: Open and Big Data (OBD), International conference on. IEEE, Los Alamitos, pp 25–30

Bastiaan M (2015) Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. In: Available at http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf

Bates DW, Leape LL, Cullen DJ, Laird N, Petersen LA, Teich JM, Burdick E, Hickey M, Kleefield S, Shea B et al (1998) Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. JAMA 280(15):1311–1316

Bennett JW, Glasziou PP et al (2003) Computerised reminders and feedback in medication management: a systematic review of randomised controlled trials. Med J Aust 178(5):217–222

Bui Q, Hansen S, Liu M, Tu Q (2018) The productivity paradox in health information technology. Commun ACM 61(10):78–85

Cachin C (2016) Architecture of the hyperledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers, vol 310

Caldicott F (2013) Information: to share or not to share? The information governance review. Department of Health, UK

Castro M, Liskov B et al (1999) Practical byzantine fault tolerance. In: OSDI, vol 99, pp 173–186

Council of European Union (2018) Council regulation (EU) no 2016/679. http://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX\%3A32016R0679. Accessed July 2018

De Montjoye Y-A, Hidalgo CA, Verleysen M, Blondel VD (2013) Unique in the crowd: the privacy bounds of human mobility. Sci Rep 3:1376

Gaur N, Desrosiers L, Novotny P, Ramakrishna V, O'Dowd A, Baset SA (2018) Hands-on Blockchain with hyperledger: building decentralised applications with hyperledger fabric and composer. Packt

Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):130

Gupta R (2018) Hands-on cybersecurity with blockchain. Packt

Hyperledger architecture (2017) Volume 1. https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf. Accessed July 2018

Hyperledger architecture (2018) Volume 2. https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf. Accessed July 2018

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system

Richard Kuhn D, Coyne EJ, Weil TR (2010) Adding attributes to role-based access control. Computer 43(6):79–81

Thakkar P, Nathan S, Vishwanathan B (2018) Performance benchmarking and optimizing hyperledger fabric blockchain platform. arXiv preprint arXiv 1805:11390

Vincent C, Hu DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K (2014) Guide to attribute based access control (ABAC) definition and considerations. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf. Accessed July 2018

Vithanwattana N, Mapp G, George C (2017) Developing a comprehensive information security framework for mhealth: a detailed analysis. J Reliab Intell Environ 3(1):21–39

Yau Wai LI, Blandford A, Cairns P, Young RM, et al (2005) Post-completion errors in problem solving

Zhang P, White J, Schmidt DC, Lenz G (2017) Applying software patterns to address interoperability in blockchain-based healthcare apps. arXiv preprint arXiv 1706:03700

Zyskind G, Oz N, et al (2015) Decentralizing privacy: using blockchain to protect personal data. In: Security and privacy workshops (SPW). IEEE, 180–184